ACIC Home

(U) Wikileaks.org—An Online Reference to Foreign Intelligence Services, Insurgents, or Terrorist Groups?

NGIC-2381-0617-08

Information Cutoff Date: 28 February 2008
Publication Date: 18 March 2008

National Security Information
Unauthorized Disclosure Subject to Criminal Sanctions

Derived from: Multiple sources
Declassify on: Source documents marked 25X1
Date of source: 20060725

This Counterintelligence Analysis Report is published under the auspices of the Department of Defense Intelligence Analysis Program (DIAP).

Prepared by:

Michael D. Horvath
Cyber Counterintelligence Assessments Branch
Army Counterintelligence Center

External Coordination: National Ground Intelligence Center[1]

This product responds to HQ, Department of Army, production requirement C764-97-0005.

ACIC Product Identification Number is RB08-0617.

[Back to Table of Contents]

(U) Purpose

(U) This special report assesses the counterintelligence threat posed to the US Army by the Wikileaks.org Web site.

[Back to Table of Contents]

(U) Executive Summary

~~(S//NF)~~ Wikileaks.org, a publicly accessible Internet Web site, represents a potential force protection, counterintelligence, operational security (OPSEC), and information security (INFOSEC) threat to the US Army. The intentional or unintentional leaking and posting of US Army sensitive or classified information to Wikileaks.org could result in increased threats to DoD personnel, equipment, facilities, or installations. The leakage of sensitive and classified DoD information also calls attention to the insider threat, when a person or persons motivated by a particular cause or issue wittingly provides information to domestic or foreign personnel or organizations to be published by the news media or on the Internet. Such information could be of value to foreign intelligence and security services (FISS), foreign military forces, foreign insurgents, and foreign terrorist groups for collecting information or for planning attacks against US force, both within the United States and abroad.

~~(S//NF)~~ The possibility that a current employee or mole within DoD or elsewhere in the US government is providing sensitive information or classified information to Wikileaks.org cannot be ruled out. Wikileaks.org claims that the "leakers" or "whistleblowers" of sensitive or classified DoD documents are former US government employees. These claims are highly suspect, however, since Wikileaks.org states that the anonymity and protection of the leakers or whistleblowers is one of its primary goals. Referencing of leakers using codenames and providing incorrect employment information, employment status, and other contradictory information by Wikileaks.org are most likely rudimentary OPSEC measures designed to protect the identity of the current or former insiders who leaked the information. On the other hand, one cannot rule out the possibility that some of the contradictions in describing leakers could be inadvertent OPSEC errors by the authors, contributors, or Wikileaks.org staff personnel with limited experience in protecting the identity of their sources.

(U) The stated intent of the Wikileaks.org Web site is to expose unethical practices, illegal behavior, and wrongdoing within corrupt corporations and oppressive regimes in Asia, the former Soviet bloc, Sub-Saharan Africa, and the Middle East. To do so, the developers of the Wikileaks.org Web site want to provide a secure forum to where leakers, contributors, or whistleblowers from any country can anonymously post or send documentation and other information that exposes corruption or wrongdoing by governments or corporations. The developers believe that the disclosure of sensitive or classified information involving a foreign government or corporation will eventually result in the increased accountability of a democratic, oppressive, or corrupt the government to its citizens.[2]

~~(S//NF)~~ Anyone can post information to the Wikileaks.org Web site, and there is no editorial review or oversight to verify the accuracy of any information posted to the Web site. Persons accessing the Web site can form their own opinions regarding the accuracy of the information posted, and they are allowed to post comments. This raises the possibility that the Wikileaks.org Web site could be used to post fabricated information; to post misinformation, disinformation, and propaganda; or to conduct perception management and influence operations designed to convey a negative message to those who view or retrieve information from the Web site.[3]

(U) Diverse views exist among private persons, legal experts, advocates for open government and accountability, law enforcement, and government officials in the United States and other countries on the stated goals of Wikileaks.org. Some contend that the leaking and posting of information on Wikileaks.org is constitutionally protected free speech, supports open society and open government initiatives, and serves the greater public good in such a manner that outweighs any illegal acts that arise from the posting of sensitive or classified government or business information. Others believe that the Web site or persons associated with Wikileaks.org will face legal challenges in some countries over privacy issues, revealing sensitive or classified government information, or civil lawsuits for posting information that is wrong, false, slanderous, libelous, or malicious in nature. For example, the Wikileaks.org Web site in the United States was shutdown on 14 February 2008 for 2 weeks by court order over the publishing of sensitive documents in a case involving charges of money laundering, grand larceny, and tax evasion by the Julius Bare Bank in the Cayman Islands and Switzerland. The court case against Wikileaks.org was dropped by Julius Bare Bank, the US court order was lifted and the Web site was restored in the United States. Efforts by some domestic and foreign personnel and organizations to discredit the Wikileaks.org Web site include allegations that it wittingly allows the posting of uncorroborated information, serves as an instrument of propaganda, and is a front organization of the US Central Intelligence Agency (CIA).[4]

~~(S//NF)~~ The governments of China, Israel, North Korea, Russia, Thailand, Zimbabwe, and several other countries have blocked access to Wikileaks.org-type Web sites, claimed they have the right to investigate and prosecute Wikileaks.org and associated whistleblowers, or insisted they remove false, sensitive, or classified government information, propaganda, or malicious content from the Internet. The governments of China, Israel, and Russia claim the right to remove objectionable content from, block access to, and investigate crimes related to the posting of documents or comments to Web sites such as Wikileaks.org. The governments of these countries most likely have the technical skills to take such action should they choose to do so.[5]

~~(S//NF)~~ Wikileaks.org uses trust as a center of gravity by assuring insiders, leakers, and whistleblowers who pass information to Wikileaks.org personnel or who post information to the Web site that they will remain anonymous. The identification, exposure, or termination of employment of or legal actions against current or former insiders, leakers, or whistleblowers could damage or destroy this center of gravity and deter others from using Wikileaks.org to make such information public.

[Back to Table of Contents]

(U) Key Judgments

- ~~(S//NF)~~ Wikileaks.org represents a potential force protection, counterintelligence, OPSEC, and INFOSEC threat to the US Army.
- ~~(S//NF)~~ Recent unauthorized release of DoD sensitive and classified documents provide FISS, foreign terrorist groups, insurgents, and other foreign adversaries with potentially actionable information for targeting US forces.
- ~~(S//NF)~~ The possibility that current employees or moles within DoD or elsewhere in the US government are providing sensitive or classified information to Wikileaks.org cannot

be ruled out. The claim made by Wikileaks.org that former US government employees leaked sensitive and classified information is highly suspect, however, since Wikileaks.org states that the anonymity of the whistleblowers or leakers is one of its primary goals.

- (U//FOUO) The Wikileaks.org Web site could be used to post fabricated information, misinformation, disinformation, or propaganda and could be used in perception management and influence operations to convey a positive or negative message to specific target audiences that view or retrieve information from the Web site.
- (U//FOUO) Several countries have blocked access to the Wikileaks.org Web site and claim the right to investigate and prosecute Wikileaks.org members and whistleblowers or to block access to or remove false, sensitive, or classified government information, propaganda, or other malicious content from the Internet.
- (U//FOUO) Wikileaks.org most likely has other DoD sensitive and classified information in its possession and will continue to post the information to the Wikileaks.org Web site.
- (U//FOUO) Web sites such as Wikileaks.org use trust as a center of gravity by protecting the anonymity and identity of the insiders, leakers, or whistleblowers. The identification, exposure, termination of employment, criminal prosecution, legal action against current or former insiders, leakers, or whistleblowers could potentially damage or destroy this center of gravity and deter others considering similar actions from using the Wikileaks.org Web site.

(U) Table of Contents

(U) Tables

(U) Figures

[Back to Table of Contents]

(U) Background

(U//FOUO) Wikileaks.org was founded by Chinese dissidents, journalists, mathematicians, and technologists from the United States, China, Taiwan, Europe, Australia, and South Africa. Its Web site became operational in early 2007. The advisory board for Wikileaks.org includes journalists, cryptographers, a "former US intelligence analyst," and expatriates from Chinese, Russian, and Tibetan refugee communities. The ACIC does not have any information to associate or link the "former US intelligence analyst" on the Wikileaks.org advisory board with the leakage of sensitive or classified DoD documents posted to the Web site.[6]

(U) Wikileaks.org claims to have developed an uncensorable version of the publicly available Wikipedia interface that is intended for mass leakage of sensitive documents that expose wrongdoing and for allowing users to comment on the documents posted to the Web site. Through its Web site, Wikileaks.org encourages large-scale anonymous leaking and posting of sensitive and confidential government and business documents on the Internet. Wikileaks.org claims to have received more than 1.2 million documents from dissident communities and anonymous sources throughout the world. If true, additional articles involving sensitive or classified DoD will most likely be posted to the Wikileaks.org Web site in the future.[7]

~~(S//NF)~~ Wikileaks.org uses its own coded software combined with Wiki, MediaWiki, OpenSSL, FreeNet, TOR, and PGP to make it difficult for foreign governments, FISS, law enforcement agencies, and foreign businesses to determine where a leaked document originated from and who was responsible for leaking the document. The goal of Wikileaks.org is to ensure that leaked information is distributed across many jurisdictions, organizations, and individual users because once a leaked document is placed on the Internet it is extremely difficult to remove the document entirely.[8]

~~(S//NF)~~ The obscurification technology[9] used by Wikileaks.org has exploitable vulnerabilities. Organizations with properly trained cyber technicians, the proper equipment, and the proper technical software could most likely conduct computer network exploitation (CNE) operations or use cyber tradecraft to obtain access to Wikileaks.org's Web site, information systems, or networks that may assist in identifying those persons supplying the data and the means by which they transmitted the data to Wikileaks.org. Forensic analysis of DoD unclassified and classified networks may reveal the location of the information systems used to download the leaked documents. The metadata, MD5 hash marks, and other unique identifying information within digital documents may assist in identifying the parties responsible for leaking the information. In

addition, patterns involving the types of leaked information, classification levels of the leaked information, development of psychological profiles, and inadvertent attribution of an insider through poor OPSEC could also assist in the identification of insiders.

(U) Wikileaks.org supports the US Supreme Court ruling regarding the unauthorized release of the Pentagon Papers by Daniel Ellsberg, which stated that "only a free and unrestrained press can effectively expose deception in government." The Wikileaks.org Web site further states the following:

> "We aim for maximum political impact. We believe that transparency in government activities leads to reduced corruption, better government, and stronger democracies. All governments can benefit from increased scrutiny by the world community, as well as their own people. We believe this scrutiny requires information. Historically that information has been costly—in terms of human life and human rights. But with technological advances—the Internet, and cryptography—the risks of conveying important information can be lowered."[10]

(U) The OPSEC measures used in the submission of leaked information to Wikileaks using the Internet are designed to protect the identity and personal security of the persons or entities sending or posting information to the Web site. Wikileaks.org claims that any attempt at trace routing of IP addresses, MAC addresses, and other identifying information of a home computer submissions (as opposed to cyber café submissions) through Wikileaks.org's Internet submission system would require a knowledge of information available only to Wikileaks.org programmers and to a rights organization serving the electronic community, or would require specialized ubiquitous traffic analysis of Internet messages and routing systems. Nevertheless, it remains technically feasible for FISS, law enforcement organizations, and foreign businesses that have the motivation, intentions, capability, and opportunity to gain online access or physical access to Wikileaks.org information systems to identify and trace whistleblowers through cyber investigations, advanced cyber tools, and forensics.[11]

(U) Another method of posting leaked information to the Web site anonymously is for leakers to use postal mail to send the information to volunteers in various countries who have agreed to receive encrypted CDs and DVDs from leakers. These volunteers then forward the information to designated personnel, who then upload the data on the CDs and DVDs to the Wikileaks.org Web servers. To protect or mask the sender, leakers can take OPSEC measures such as using Wikileaks.org encryption protocols when writing CDs and DVDs; using gloves while wrapping, taping, handling, and mailing packages; and not including a return address or including a fake return address on packages containing leaked information. Such measures are designed to protect the identity of the leakers and prevent FISS, law enforcement, and postal inspectors from intercepting the mail and decoding the information on the data storage devices in transit. Wikileaks.org also claims that it is developing easy-to-use software to encrypt the CDs and DVDs. Use of such methods also protects facilitators or intermediaries from harm because they would not know the content of the encrypted submissions.[12]

(U) A Wikileaks.org spokesperson stated in early January 2007 that about 22 persons are involved in the Open Society Initiative to make governments and corporations more accountable

to the citizens of the world. Wikileaks intends to seek funding from individual persons and groups such as humanitarian organizations that fund sociopolitical activity intended to promote democracy and human rights around the world through open access to government and business information.[13]

~~(S//NF)~~ Several foreign countries including China, Israel, North Korea, Russia, Vietnam, and Zimbabwe have denounced or blocked access to the Wikileaks.org Web site to prevent citizens or adversaries from accessing sensitive information, embarrassing information, or alleged propaganda. The governments of China, Israel, and Russia have asserted that they have a right to remove from the Internet protected government information, disinformation, and propaganda that is intended to embarrass or make false allegations against their governments. China, Israel, North Korea, and Russia are assessed to have state-sponsored CNE, computer network attack (CNA), and cyber forensics capabilities that would most likely allow penetration or disrupt viewing of the Wikileaks.org Web site. China, Israel, and Russia have used or are suspected of having used CNA to target terrorist or dissident Web sites that have posted objectionable material intended to embarrass, harm, or encourage terrorism or opposition to the government.[14]

[Back to Table of Contents]

(U) Discussion

(U//FOUO) An insider could present a potential force protection, counterintelligence, OPSEC, or INFOSEC threat to the US Army through deliberate unauthorized release of official DoD documents and posting of sensitive or classified information to the Internet. Several recent postings to the Wikileaks.org Web site in November 2007 of sensitive US Army information marked UNCLASSIFIED//FOR OFFICIAL USE ONLY and in December 2007 of US Army information classified SECRET//NOFORN highlight the insider threat to DoD. The actual perpetrators responsible for the unauthorized released of such documents could be subject to administrative action, nonjudicial punishment, or criminal charges and prosecution if they are identified.

(U) Wikileaks.org Analysis of US Army Tables of Equipment in Iraq and Afghanistan from April 2007

(U) Wikileaks.org specifically cited 2,000 pages of leaked US Army documents with information on the Tables of Equipment (TOEs) for US and Coalition forces in Iraq and Afghanistan as a perfect example of the sort of information that would benefit from a global analysis. These documents provided information on the US forces, a description of equipment and total number of equipment that were assigned to actual military units assigned to US Central Command in April 2007. Wikileaks.org staff members and various authors and contributors have written numerous news articles and posted the raw data in spreadsheets or Structured Query Language (SQL) data base so anyone can examine the information, conduct research, comment upon, discuss the various units, see the items of equipment, see what they do, and draw their own conclusions about the strategic, political, military, and human rights significance of the information.[15]

(U//FOUO) *Table 1* below is an abbreviated sample of information contained in a leaked digital database document or spreadsheets available on the Wikileaks.org Web site:

[Back to Table of Contents]

(U) Table 1. Abbreviated Listing of the Iraq Transition Team (UIC - M94216) Table of Equipment (TOE). [16]

UIC	LIN	NSN	Item Name	PBIC	Type	DND	Qnty
M94216	72045Z	581001X111125	WARLOCK GREEN, ECM: GREEN EDO CO	V	TPE	N	15
M94216	72113Z	581001X111126	WARLOCK RED, ECM: RED EDO COMM &	T	TPE	N	2
M94216	72113Z	581001X111126	WARLOCK RED, ECM: RED EDO COMM &	V	TPE	N	13
M94216	B67766	1.24001E+12	BINOCULA MOD CN M22	N	TPE	N	9
M94216	E63317	6.60501E+12	COMPAS MAGNETIC UNMTD	P	TPE	N	3
M94216	J03261	5.85501E+12	ILLUMI INFR AN/PEQ-2A	P	TPE	N	6
M94216	J85705	8.47002E+12	INSERTS,ENHANCED SM	N	TPE	N	4
M94216	J85705	8.47002E+12	INSERTS,ENHANCED SM	N	TPE	N	49
M94216	J85705	8.47002E+12	INSERTS,ENHANCED SM	N	TPE	N	8
M94216	J85705	8.47002E+12	INSERTS,ENHANCED SM	N	TPE	N	49
M94216	L91975	1.005E+12	MG 50 M2 HB FL GD/VEH	P	TPE	N	3
M94216	L92352	1.00501E+12	MACH GUN 7.62MM M240	N	TPE	N	2
M94216	M09009	1.00501E+12	MACH GUN 5.56MM M249	P	TPE	N	3
M94216	M74823	1.01001E+12	MT MACH GUN MK64 MOD9	T	TPE	N	1
M94216	M75577	1.005E+12	MT TPD MG CAL .50 M3	P	TPE	N	1
M94216	M92841	1.00501E+12	MACH GUN 7.62MM M240B	N	TPE	N	2
M94216	M92841	1.00501E+12	MACH GUN 7.62MM M240B	T	TPE	N	2
M94216	N05482	5.85501E+12	NIGHT VIS G AN/PVS-7B	P	TPE	N	8
M94216	T92446	2.32001E+12	TRK UTIL HMMWV M1114	T	TPE	N	1
M94216	W95537	2.33001E+12	TRL CGO 3/4T M101 2WH	T	TPE	N	3
M94216	YF2014	232001C043031	HMMWV M1114: W/ OFK5	T	TPE	N	2
M94216	YF2049	2.32001E+12	TRUCK,UTILITY-(M1116)	T	TPE	N	1
Legend:							

UIC – Unit Identification Code, a six-character, alphanumeric code that uniquely identifies each Active, Reserve, and National Guard unit of the US Armed Forces.

LIN – Line Item Number for equipment.

NSN – NATO Stock Number, a standardized stack identification number for supplies and equipment within the North Atlantic Treaty Organization).

Item Name - Brief description of the equipment.

PBIC – Property Book Identification Code, which categorizes the type of property listed into one of 10 categories.

Type (of equipment):

> TPE – Theater Provided Equipment; specific equipment that is provided by the Theater of Operations such as CENTCOM to perform the mission based on the unique operating environment
>
> LTT – Long Term Training; equipment need for long term training or deployment.
>
> APS – Army Prepositioned Stock; equipment drawn by a unit that is already prepositioned in the Theater of Operations.

DND – Do Not Deploy; this field is a Yes/No column that lists equipment that remains at the home station and is not deployed with the unit when sent overseas.

OH Qty – On-hand Quantity is the number of item of equipment that is currently available to the unit; it does not necessarily represent the actual required number needed by the unit to be fully mission capable.[17]

UNCLASSIFIED//FOR OFFICAL USE ONLY

~~(S//NF)~~ The foreign staff writer for Wikileaks.org, Julian Assange, wrote several news articles, coauthored other articles, and developed an interactive data base for the leaked documents. In addition, other Wikileaks.org writers and various writers for other media publications wrote separate news articles based on the leaked information posted to the Web site. Assange and his coauthors claim that the 2,000 pages of leaked US military information provides unit names, organizational structure, and tables of equipment (TOEs) for the US Army in Iraq and Afghanistan. They also claimed that unidentified persons within the US government leaked the information to facilitate action by the US Congress to force the withdrawal of US troops by cutting off funding for the war.[18]

(U//FOUO) Assange and other Wikileaks.org writers purport that the leaked sensitive TOE information reveals the following:

- Secretive US document exploitation centers.
- Detainee operations and alleged human rights violations.
- Information on the US State Department, US Air Force, US Navy and US Marines units, Iraqi police and coalition forces from Poland, Denmark, Ukraine, Latvia, Slovakia, Romania, Armenia, Kazakhstan, and El Salvador serving in Iraq and Afghanistan.
- Nearly the entire order of battle for US forces in Iraq and Afghanistan as of April 2007.
- Alleged revelations that the US government violated the Chemical Weapons Convention in Iraq and Afghanistan.[19]

~~(S//NF)~~ Wikileaks.org encouraged persons to comment on the leaked Army documents and explained how the catalogued information and cross-referenced databases could be used by other researchers or journalists to prepare reports or assessments. According to Wikileaks.org, the information posted can be used to prepare objective new reports. Conversely, this same information could be manipulated to prepare biased news reports or be used for conducting propaganda, disinformation, misinformation, perception management, or influence operations against the US Army by a variety of domestic and foreign actors. [20]

(U) Assange and other Wikileaks.org writers developed and applied a specific methodology for examining and analyzing the leaked TOE information, a methodology they then placed online to assist others in conducting their own research. *See Appendix B.* They also provided links to associated online reference material. The methodology used by Assange and other authors for the analysis of leaked tables of equipment for US Forces in Iraq and Afghanistan both a SQLite database is described in *Appendix B.*

~~(S//NF)~~ The TOEs for US Army units deployed to Afghanistan and Iraq in April 2007 provide a wealth of information that could be used by FISS, foreign terrorist groups, and Iraqi insurgents to identify unit capabilities and vulnerabilities that could assist in conducting attacks against camps, convoys, and other targets. The information can also be compared with other publicly available databases to develop extensive order of battle files of vehicle types, communications and jamming equipment, information systems, and weapons systems, files that could be used to determine the capabilities, limitations, and vulnerabilities of the organic equipment assigned to military units. Such information could aid enemy forces in planning terrorist attacks, selecting the most effective type and emplacement of improvised explosive devices (IEDs), building triggering devices to defeat countermeasures organic to friendly units, and selecting the most effective direct and indirect weapons systems for conducting physical attacks against targets such as military units, convoys, and base camps.

(U) One Wikileaks.org news article also discusses the use of IEDs by foreign terrorists and insurgent groups and claims that the IED threat has resulted in a shift in DoD funding priorities, similar to the Manhattan Project to develop atomic weapons in World War II, for current research, development and fielding of IED countermeasures through the Joint IED Defeat Organization. In addition, the author of the article attempts to provide a cost-to-benefit analysis of these IED tactics and countermeasures. The author claims that the leaked information reveals that 12,097 Warlock, Counter RCIED (Remote-controlled Improvised Explosive Device) Electronic Warfare (CREW), systems are in Iraq and that the purpose of the Warlock is to jam radio signals from devices such as mobile phones to prevent such signals from detonating IEDs.

The author claimed that 7,530 systems used in Iraq were purchased at a cost of $1.1 billion. No claim was made regarding the cost of remaining 4,567 systems.

~~(S//NF)~~ The author of the above-mentioned article incorrectly interprets the leaked data regarding the components and fielding of the Warlock system, resulting in unsupportable and faulty conclusions to allege war profiteering, price gouging and increased revenues by DoD contractors involved in counter-IED development efforts. This article provides an example of how the leaked TOE information can be manipulated and misinterpreted to produce inaccurate information for a news article.

~~(S//NF)~~ The author of the article then argues that the US Army receives a poor return on its investment in counter-IEDs. The following excerpt from the article could be used by adversaries in potential propaganda or influence operations:

> If we view IEDs as a rebel investment, to which the United States must pay dividends in defensive equipment costs, then every insurgent dollar spent has a return on investment of somewhere around a thousand fold. Significant price gouging by counter-IED defense contractors is evident. For comparison, each briefcase-sized "Warlock" IED jammer, of which is there is on average more than one per vehicle, is worth $150,000; however, as can be seen by this analysis that is more costly than nearly every vehicle it was designed to protect. The "Warlock" producer, a DoD defense contractor [name redacted], predicts financial year 2007 will see a 400 percent total revenue increase over its 2003 levels.[21]

~~(S//NF)~~ Intelligence indicates that insurgents in Afghanistan have recovered several Warlock systems.[22] It is possible that Warlock systems captured in Afghanistan were sent to Iran for reverse engineering and for use in developing countermeasures to Warlock.

~~(S//NF)~~ Were a Warlock system successfully reversed engineered or countermeasures successfully developed by foreign terrorists, insurgents, or the Iranian government, US and Coalition forces would be at greater risk of RCIED attacks, especially those units equipped with Warlock systems similar to those that had been captured and exploited. It is also possible that any countermeasures developed to defeat the Warlock system would be provided to the Jaysh al-Mahdi (JAM) and other anti-US insurgent or terrorist groups operating in Iraq and Afghanistan. The TOEs could be used to identify and target specific units equipped with the same type of Warlock systems for which countermeasures had been developed.

(U) The Wikileaks.org authors believe that the leaked documents list Army equipment held by the US Army, Marines, Air Force, Coalition, and possibly CIA units in Iraq and Afghanistan as of April 2007. The authors stated that the data only includes items registered with battle planning systems for logistics and appears to cover most valuable major end items of equipment. The data, according to the authors, does not include soldiers' combat pay, transportation, research and development, and home station costs of the soldiers, nor does it include most supplies, ammunition, and other disposable equipment and consumable items.[23]

(U) Wikileaks.org staff personnel allegedly wrote a script or computer program to cross reference each item in the leaked document with NSNs gleaned from public US logistics equipment price catalogs from the Defense Logistics Agency (DLA). The authors claim that $1.112 billion worth of US Army-managed military equipment in Afghanistan is listed in the leaked documents. The author believed the actual total value of the equipment to be several times higher.[24]

(U) The spreadsheets and list contains codes to identify military units, supply item codes, and other logistics data. The authors believed that the most useful data field for investigatory purposes was the NSN. The authors found several Internet sites that allow public searches of the NSNs, and this information was merged with the TOE into the SQL-generated database on the Web site. For example, the author specifically mentioned NSN catalogues that are publicly available on the Internet from the DLA.[25] The DLA Web site identifies many items on the spreadsheets and includes prices that were merged into the database and used to generate the estimate for the total value of the equipment.[26]

(U//FOUO) Julian Assange also stated in his news articles involving the TOE information that persons were welcome to assist in the following future actions and areas of research involving the equipment listings:

- A computer program would be written to expand the military unit abbreviations (for example, HHC—Headquarters and Headquarters Company) to make is easier for users to visually analyze entries in the database.
- Make further comments on military units in the list and their significance. The entries would be cross linked with available news sources.
- Make further comments on equipment items in the list and their significance.
- Expand and improve links and other information for US war-funding legislation and bills.
- Attempt to answer questions on specific issues with NSN codes. The authors stated that the NSNs are a 13-digit code. Of those 13 digits, 12 are numeric. The seventh is alphanumeric, and the publicly searchable NSN database seems to be able to locate items if they have a number in the seventh place, but, not if there is a letter in the seventh place. They ask the following questions: 1) What is the significance for this alphanumeric character in the seventh position? 2) What does a letter as opposed to a number signify? 3) Is there a more complete public database for NSN codes than the one given? 4) Are these alphanumeric NSNs Management Control Numbers as speculated?
- Create an interactive database browser.[27]

(U) Julian Assange and other Wikileaks.org authors continually encourage other persons with an interest in the information to comment on their work or conduct their own research and publish the results on Wikileaks.org.

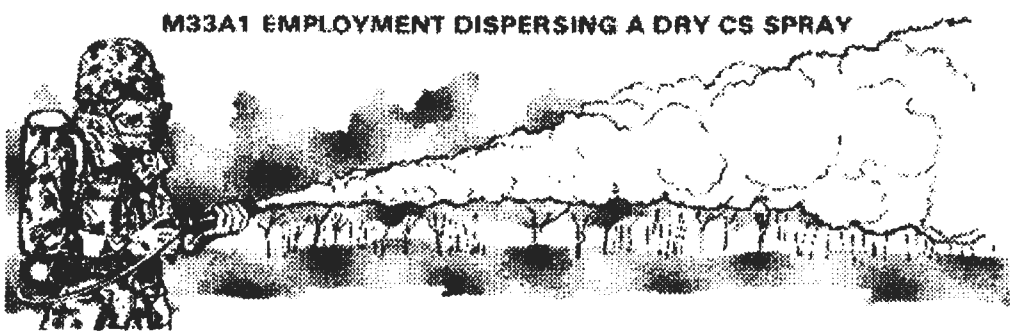
(U) Alleged Violations of the Chemical Warfare Convention Treaty by US Military in Iraq and Afghanistan

(U) On 9 November 2007, Wikileaks.org published an exclusive investigative report claiming that the United States "had almost certainly violated the Chemical Weapons Convention"

(CWC), as originally drafted by the United Kingdom in 1997. The author, Julian Assange, claimed the deployment of CS (2-chlorobenzalmalononitrile also called Chlorobenzylidene Malononitrile) munitions and dispensing equipment and weapons capable of firing CS gas by the United States was a violation of the CWC. The author also claimed the United States had at least 2,386 low-grade chemical weapons deployed in Iraq and Afghanistan. These items also appeared in the 2,000-page listing of nearly one million items of US military equipment deployed in Iraq and leaked to Wikileaks.org. The items are labeled under the military's own NATO supply classification for chemical weapons and equipment.[28]

(U) Prior to the invasion of Iraq in 2003, the Defense Department released an official statement that President Bush had authorized US military forces to use riot control agents (RCAs) such as tear gas or CS gas. *See Figure 1.* The Defense Department stated that tear gas or CS gas, which was issued to US troops, would be used only to save civilian lives and in accordance with the CWC, as amended and ratified by the United States. Some chemical weapons experts in the United States and other countries expressed the belief that this 2003 authorization might violate the CWC treaty. These domestic and foreign critics expressed the belief that any battlefield use of tear gas would violate the CWC; offend crucial allies, including the United Kingdom and Australia. In addition, the critics claimed that the usage of CS would provide the Iraqi leader, Saddam Hussein, a pretext for using chemical weapons against the United States and coalition forces.[29]

UNCLASSIFIED



(U) Figure 1. M33A1 Bulk CS Chemical Dispenser.

[Back to Table of Contents]

(U//FOUO) In the report published on Wikileaks.org, the author claimed that any use of chemical weapons such as CS gas for military operations is illegal. The Chemical Weapons Convention of 1997, drafted by the United Kingdom declares "Each State Party undertakes not to use riot control agents as a method of warfare." It only grants permissible use to "law

enforcement including domestic riot control." The authors used this interpretation of the CWC drafted by the United Kingdom to make the allegation that the United States had violated the treaty. [30]

(U//FOUO) It must be noted, that US policy as stated in Executive Order No. 11850, 8 April 1975, *Renunciation of Certain Uses in War of Chemical Herbicides and Riot Control Agents*, renounced first use of herbicides in war (except for specified defensive uses) and first use of RCAs in war except for defensive military modes to save lives. In ratifying the CWC, the US Senate wrote an amendment into its resolution approving the CWC that stated United States' interpretation of how RCAs might be used for specific defensive purposes, as specified by the 1975 Executive Order.[31]

(U) Such varying interpretations reflect a deliberate ambiguity in the CWC, which states that "riot-control agents may not be used as a method of warfare." The original CWC and modified CWC approved by the US Senate, however, does not define this phrase "method of warfare." The actual version of the CWC passed by the US Senate was not considered by the authors of the report. The CWC ratified by the US Senate list exceptions in the usage of RCAs for US military forces that are not considered by the US government to be in violation of the CWC.[32]

(U) In the same report, the authors claimed that the use of white phosphorus by the US military during the 2004 assault on Fallujah, Iraq, should also be considered a violation of the CWC. The authors noted, however, that the US Army claimed usage of white phosphorous as "a smoke screen" and "an incendiary" in the Fallujah operation, and that this usage is not technically covered by the CWC.

(U) Alleged Human Rights Violations Related to Joint Task Force–Guantanamo Standard Operating Procedures

(U//FOUO) Another example of leaked information posted to the Wikileaks.org Web site on or about 7 November 2007 is an outdated copy of the Joint Task Force–Guantanamo, Camp Delta Standard Operating Procedures (SOP) marked as UNCLASSIFIED//FOUO, signed by MG Miller and dated 28 March 2003. A news article written by Wikileaks.org staff writers, also posted on 7 November 2007, claims the SOP exposes systematic methods for preventing illegal combatants and detained prisoners incarcerated at Joint Task Force–Guantanamo facilities at Camp Delta from meeting with the International Red Cross, as well as the use of extreme psychological stress as a means of torture against detainees. The unauthorized release of the SOP has prompted authors posting to the Wikileaks.org Web site to claim that the document proves the US Army was torturing and violating the human rights of detainees held at Guantanamo Bay. This SOP was also the subject of a lawsuit by international human rights groups and a domestic civil rights organization requesting the release of the document under the US Freedom of Information Act.[33]

(U) The author claimed that subsequent US military statements including a DoD spokesperson, to Reuters News Service and the *Miami Herald* confirm the veracity of the JTF SOP document. On Wednesday, 14 November 2007, a week after the SOP was posted to Web site, Wikileaks.org claimed that it received an e-mail message from the "Pentagon" (DoD) demanding that the

documents posted to the Web site be censored and removed from the Web site. The actual wording of the DoD e-mail message sent to Wikileaks.org requested that the document be removed from the Web site and that the procedures under the Freedom of Information Act be used to request release of the SOP.[34]

(U) Leakage of Classified Information to Wikileaks.org

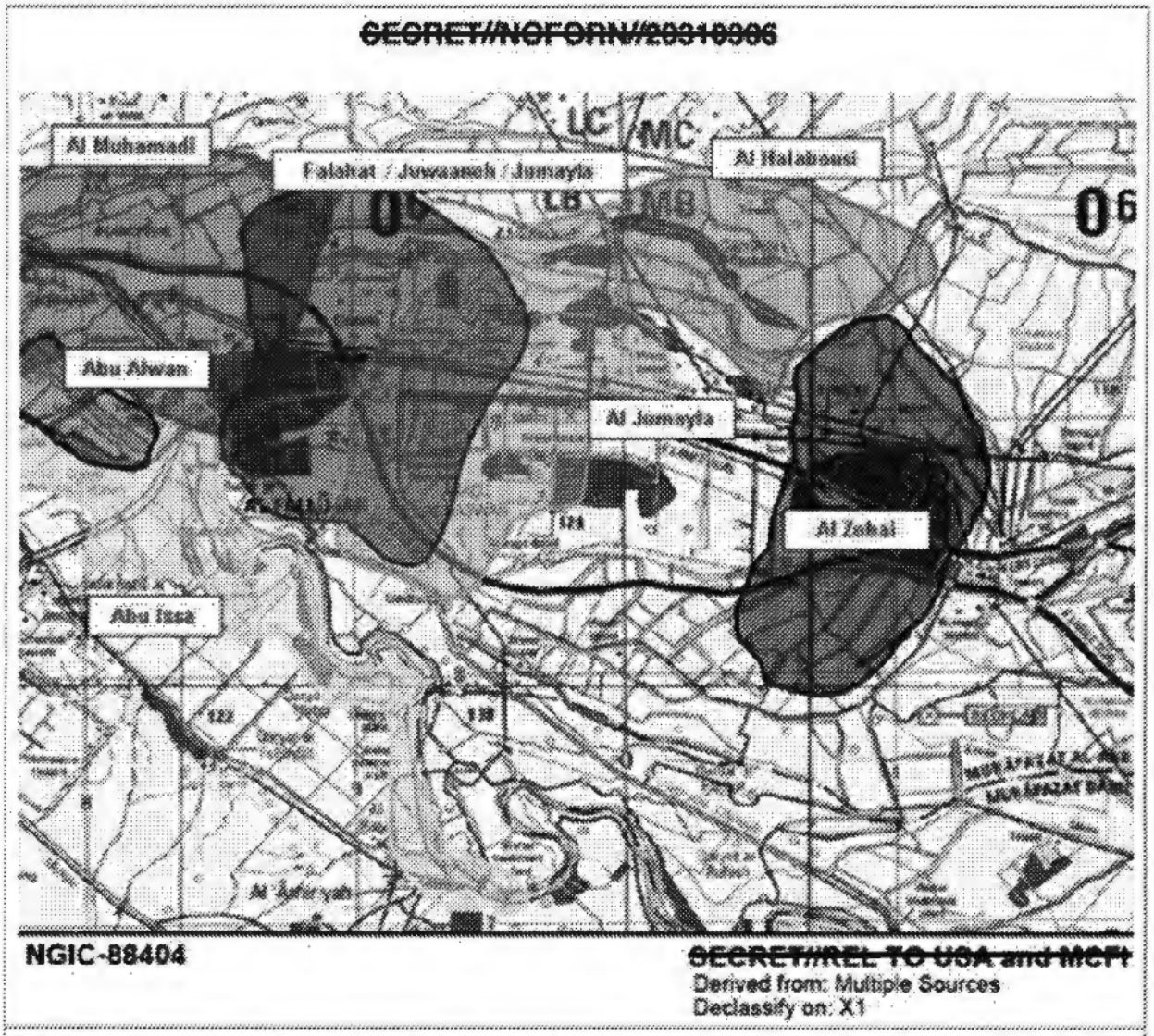
~~(S//NF)~~ Wikileaks.org also posted a report by the National Ground Intelligence Center (NGIC), classified SECRET//NOFORN, entitled " *(U) Complex Environments: Battle of Fallujah I, April 2004,"* (NGIC-1127-7138-06). The NGIC report was the second in a series of reports that analyzed recent warfare in complex environments such as urban environments. *See Figure 2.* The NGIC report discusses enemy use of asymmetric tactics, techniques, and procedures (TTP) during the Battle of Fallujah in April 2004 and offers many useful lessons learned regarding how a relatively weak adversary can prevent the United States from accomplishing its military objectives. Wikileaks.org claims the document was leaked by a source it refers to as "Peryton," who is described as a former employee of NGIC. Both a copy of the actual NGIC classified report (in PDF) and the Wikileaks.org news article were posted on the Wikileaks.org Web site. A variety of newspapers, wire services, and other news and media organizations wrote numerous articles based on the original Wikileaks.org news article and actual classified document posted to their Web site.[35]

~~(S//NF)~~ The possibility that a current employee or mole may exist within DoD or elsewhere in the US government who is actively providing sensitive or classified information to Wikileaks.org cannot be ruled out. Nevertheless, the claim that the leaker is a former NGIC employee is highly suspect, since Wikileaks.org claims that the protection of the anonymity of the "whistleblower" or "leaker" is one of its primary concerns. In addition, this claim could simply be a crude attempt to mislead investigations into who leaked the document. Use of a code name, incorrect employment information, or incorrect status are most likely rudimentary OPSEC measures designed to protect the identity of the current or former "insider" who leaked the information. In addition, usage of present and past verb tenses and other contradictions in referencing "Peryton" by the Wikileaks author and staff personnel are most likely part of a deliberate deception, but one cannot completely rule out the possibility that some of these contradictions could be inadvertent OPSEC errors made by authors lacking experience in protecting their methods or sources.

~~(S//NF)~~ Unclassified e-mail addresses and work telephone numbers of the authors and other persons referenced in the NGIC report were listed in the NGIC document, thus making them available to members of the news media attempting to verify the leaked information. Wikileaks.org and some other news organizations did attempt to contact the NGIC personnel by e-mail or telephone to verify the information. Such efforts by Wikileaks.org to verify the information are in contravention to its stated policy not to attempt to verify the information it receives from its sources. Wikileaks.org went forward with publishing their news article based on the classified NGIC report although they did not receive a response to their inquiry. This is of interest because some journalists exploit the lack of a response to their inquiries by implying that a refusal to respond, failure to respond to a FOIA request, or failure to verify or receive other information presumes that those failing to respond have something to hide. This further weakens

the claim that an alleged former NGIC employee leaked the information and strengthens other possibilities. A former NGIC employee would be regarded by many as a highly credible source and either taken at his or her word or asked to provide other bona fides to verify the employment claim. Given the high visibility and publicity associated with publishing this classified report by Wikileaks.org, however, attempts to verify the information were prudent and show journalist responsibility to the newsworthiness or fair use of the classified document if they are investigated or challenged in court.[36]

~~SECRET//NOFORN~~



(U) The following is a description of the map and explanation of the classification markings provided in the Wikileaks.org article: "Map from page four of the leaked report on the failed 2004

assault on the Iraqi town of Fallujah, which is situated 40 miles from Baghdad. The report is classified SECRET/NOFORN. NOFORN means do not share with US allies such as the UK, Australia, and Canada. 20310603 is date after which 25 years have elapsed and the document would normally be declassified. X1 specifies that the document is exempt from declassification."

~~(S//NF)~~ Figure 2. Map from Page 4 of NGIC Report Entitled "*(U) Complex Environments: Battle of Fallujah I, April 2004*" As Published in a Wikileaks.org Article.

[Back to Table of Contents]

~~(S//NF)~~ The author on the Wikileaks.org staff published the article using selected excerpts and used information that was out of context from the actual NGIC report. The article intertwined classified information from the NGIC report and information gleaned from other news articles in the open media to strengthen its portrayal of the coalition offensive operations in Fallujah in 2004 as a military and political defeat for the United States. The leakage of this NGIC report could allow anti-Coalition forces to portray themselves as victors because they successfully manipulated the media coverage in the April 2004 battle to divide the coalition forces politically and force a halt to the offensive operations. The leaked report could also provide foreign governments, terrorists, and insurgents with insight into successful asymmetric warfare tactics, techniques, and procedures that could be used when engaging US or Coalition forces and provide insight into effective media, information, or influence operations that could be used to defeat a superior enemy.[37]

(U) The catalogue, indexing and filing entry on the Wikileaks.org Web site for the leaked NGIC document is in *Table 2*, below. This is the information as posted on the Wikileaks.org Web site.

[Back to Table of Contents]

~~(S//NF)~~ Table 2. Descriptive Entry of the File and How it is Catalogued by Wikileaks.org for the NGIC Report Entitled "*(U) Complex Environments: Battle of Fallujah I, April 2004*" [NGIC-1127-7138-06], as Posted on its Web Site.[38]

File	fallujah.pdf (click to view file)
Analysis	Al Jazeera and Abu Ghraib scuttled US war in Fallujah
Summary	Classified 2006 SECRET//NOFORN report by the US Army National Ground Intelligence Center. "Enemy employment of asymmetric tactics, techniques, and procedures (TTP) during the Battle of Fallujah in April 2004 offers many useful lessons learned in how a relatively weak adversary can prevent the United States from accomplishing its military objectives."

File Size	280144K
File Info	PDF document, version 1.4
File Identity	SHA256 28d7b0d27805749db32f38088c9ecbb963d4564877e723930cf44d8d0c6c7c8e
Wikileaks release	2007-12-24
Country	United States
Organization	US Army National Ground Intelligence Center
Organization type	Military or intelligence (ruling)
Submitted by	Peryton [**ACIC comment:** this is the code name given by Wikileaks.org to the leaker(s) of the information.]

~~SECRET//NOFORN~~

(U) Technical Skills and Abilities

~~(S//NF)~~ Wikileaks.org developers and technical personnel appear to demonstrate a high level of sophistication in their efforts to provide a secure operating environment for whistleblowers desiring to post information to the Web site. They currently use a variety of indigenously modified free software to build the Web site and route and secure the transmission of data to Wikileaks.org.

~~(S//NF)~~ The construction of a SQL database, the merging of leaked documents, and use of publicly available tools to glean information from the Web sites of various DoD and private organizations such as globalsecurity.org and then make the information available in a searchable format, allowing access to and manipulation of the data and information for research purposes by users of Wikileaks.org, demonstrate a high level of technical capability and resourcefulness.

~~(S//NF)~~ The current and future intent of the Wikileaks.org staff and writers is to continue development of enhanced tools for the manipulation of the 2,000 pages of information on US forces by visitors to the Web site. Future efforts may include expanding the use of encryption, operational cyber tradecraft, and physical tradecraft in the delivery and transmission of leaked information for posting to the Wikileaks.org Web site. It is highly likely that transmission security will improve as new technology, the technical skills of current members, or new funding sources allow. The purchase of more secure equipment, transmission means, and encryption protocols is possible if additional financial resources are made available to the organization.

(U) Is it Free Speech or Illegal Speech?

(U//FOUO) Wikileaks.org allows anonymous publication of information and records without oversight or accountability; anyone can post information to the Web site, and there is no editorial review, fact checking, or oversight of the posted information. Persons accessing the Web site are encouraged to form their own opinions regarding the accuracy of the information and are

allowed to post their own comments. This open policy of posting information and providing commentary could create multiple legal issues for Wikileaks.org that could subject members to legal prosecution or civil issues by foreign governments, businesses, and individual complainants. In addition, some governments may contend that accessing the Web site itself is a crime, and that shutting down or blocking access to the Web site is a reasonable countermeasure to prevent viewing or downloading of objectionable content. This situation raises the possibility that the Wikileaks.org Web site could be deliberately used to post fabricated information; to post misinformation, disinformation, or propaganda; or to conduct perception management and influence operations designed to convey a negative message to specific audiences.

(U) Diverse views exist within the United States and other countries regarding the stated goals of Wikileaks.org. Some believe that the leaking and posting of information is constitutionally protected free speech and supports freedom of the press, open-society initiatives, and government accountability, and that leaking the information serves the greater good versus any illegal acts that arise from the posting of sensitive or classified government or business information. Others believe that Wikileaks.org or individual persons associated with Wikileaks.org will face legal challenges in some countries regarding the privacy of individuals and businesses, the revelation of sensitive or classified government information, or the posting of information that is allegedly wrong, false, slanderous, or libelous. Several foreign companies have already filed civil lawsuits in the United States and the United Kingdom for data theft, libel, and damage to their business reputation for the posting of internal and proprietary company information to the Wikileaks.org Web site. The Wikileaks.org Web site was temporarily shutdown in late February 2008 for 2 weeks in the United States by court order over the publication of sensitive documents in a case involving a potential money laundering, grand larceny, and tax evasion charges by the Julius Bare Bank in the Cayman Islands and Switzerland. Julius Bare Bank decided to drop the court case against Wikileaks.org in US courts. The US court order was lifted and the Web site was restored in the United States.

(U) In addition, several prominent bloggers have questioned the usage and reliability of the security of the software used to develop the Web site and to protect communications and identities of leakers. The motives and methods of the Wikileaks.org developers and members have been questioned, and several bloggers believe that other Internet forums exist that served the same function in a more ethical manner. Efforts by some domestic and foreign personnel to discredit the Wikileaks.org Web site include allegations that it allows uncorroborated information to be posted, serves as an instrument of propaganda, and is a front organization for the Central Intelligence Agency (CIA). Wikileaks.org denies these accusations, and no evidence has been presented to support such assertions.[39]

(U//FOUO) Questions and concerns have been raised by media consultants, ethics experts, and other journalists regarding the status of Wikileaks.org as a news organization and of its staff writers as journalists. The contention by some is that Wikileaks.org does not qualify as a news organization and thus its staff writers are not journalists. Wikileaks.org's desire to expose alleged wrongdoing by revealing sensitive or classified government or business information, in effect, encourages the theft of sensitive or classified proprietary information or intellectual property. In doing so, some argue, Wikileaks.org is knowingly encouraging criminal activities such as the theft of data, documents, proprietary information, and intellectual property, possible violation of

national security laws regarding sedition and espionage, and possible violation of civil laws. Within the United States and foreign countries the alleged "whistleblowers" are, in effect, wittingly violating laws and conditions of employment and thus may not qualify as "whistleblowers" protected from disciplinary action or retaliation for reporting wrongdoing in countries that have such laws. Also, the encouragement and receipt of stolen information or data is not considered to be an ethical journalistic practice. In addition, the sources of Wikileaks.org staff writers are not verified, nor are its news articles fact-checked or confirmed by additional sources, as customary in news organizations. Moreover, there is no editorial review of the articles prior to publication. Finally, some critics contend that the staff writers are biased and have made unsupportable claims to support political agendas to effect change in government or business policy.[40]

(U) Several countries have complained publicly or blocked access to Wikileaks.org and similar Web sites and have asserted claims that they have the right to investigate and prosecute Wikileaks.org members and whistleblowers. In addition, several countries also claim the right to remove false information, sensitive or classified government information, propaganda, or other malicious content from the Internet. As a result, Wikileaks.org members have already posted information in China on how to circumvent blocks to the Web site imposed by the Chinese government for having objectionable content related to the participation of Chinese dissents in Wkileaks.org and to pro-democracy issues. [41]

[Back to Table of Contents]

(U) Intelligence Gaps

- ~~(S//NF)~~ What individual persons or entities are leaking DoD sensitive or classified information to Wikileaks.org, and are they working on behalf of a foreign agent or power? What are the reasons, intentions, and motivations of the current or former insider?
- ~~(S//NF)~~ Is the potential insider leaking the information to Wikileaks.org a former employee of the US government or a mole still working for the US government? How is the insider sending digital information to Wikileaks.org? What cyber or other tradecraft is the perpetrator using?
- ~~(S//NF)~~ Will the Wikileaks.org Web site be used by FISS, foreign military services, foreign insurgents, or terrorist groups to collect sensitive or classified US Army information posted to the Wikileaks.org Web site?
- ~~(S//NF)~~ Will the Wikileaks.org Web site be used by FISS, foreign military services, or foreign terrorist groups to spread propaganda, misinformation, or disinformation or to conduct perception or influence operations to discredit the US Army?
- ~~(S//NF)~~ Will the Wikileaks.org Web site be used for operational or cyber tradecraft to pass information to or from foreign entities?
- ~~(S//NF)~~ Will the Wikileaks.org Web site developers obtain new software for Web site development, management, security, encryption of messages or files, or posting anonymous information to the Web site?
- ~~(S//NF)~~ From what foreign personnel or groups does Wikileaks.org receive funding or collaborate with for sharing information or development of new software?

- ~~(S//NF)~~ Will foreign entities attempt to conduct CNE or CNA to obtain information on the posters of information or block content on the Wikileaks.org Web site?
- ~~(S//NF)~~ What software, tactics, techniques, and procedures would be used by a foreign actor to conduct CNE or CNA against the Web site?
- ~~(S//NF)~~ Will foreign persons, businesses, or countries attempt civil lawsuits or criminally prosecute whistleblowers, Wikileaks.org staff, and members who posted comments on the Web site?
- ~~(S//NF)~~ Will Wikileaks.org and various users expand the data fields in the TOE SQL database to include equipment capabilities, equipment limitations and vulnerabilities, known unit locations, links to geospatial information services, or known unit personnel to develop "battle books" for targeting packages?
- ~~(S//NF)~~ What other leaked DoD sensitive or classified information has been obtained by Wikileaks.org?
- ~~(S//NF)~~ Will foreign organizations such as FISS, foreign military services, foreign insurgents, or terrorist groups provide funding or material support to Wikileaks.org?

[Back to Table of Contents]

(U) Conclusions

~~(S//NF)~~ Web sites such as Wikileaks.org have trust as their most important center of gravity by protecting the anonymity and identity of the insider, leaker, or whistleblower. Successful identification, prosecution, termination of employment, and exposure of persons leaking the information by the governments and businesses affected by information posted to Wikileaks.org would damage and potentially destroy this center of gravity and deter others from taking similar actions.

(U//FOUO) The unauthorized release of DoD information to Wikileaks.org highlights the need for strong counterintelligence, antiterrorism, force protection, information assurance, INFOSEC, and OPSEC programs to train Army personnel on the proper procedures for protecting sensitive or classified information, to understand the insider threat, and to report suspicious activities. In addition, personnel need to know proper procedures for reporting the loss, theft, or comprise of hard or soft copy documents with sensitive information or classified information to the appropriate unit, law enforcement, or counterintelligence personnel. Unfortunately, such programs will not deter insiders from following what they believe is their obligation to expose alleged wrongdoing within DoD through inappropriate venues. Persons engaged in such activity already know how to properly handle and secure sensitive or classified information from these various security and education programs and has chosen to flout them.

~~(S//NF)~~ It must be presumed that Wikileaks.org has or will receive sensitive or classified DoD documents in the future. This information will be published and analyzed over time by a variety of personnel and organizations with the goal of influencing US policy. In addition, it must also be presumed that foreign adversaries will review and assess any DoD sensitive or classified information posted to the Wikileaks.org Web site. Web sites similar to Wikileaks.org will continue to proliferate and will continue to represent a potential force protection, counterintelligence, OPSEC, and INFOSEC threat to the US Army for the foreseeable future.

Sensitive or classified information posted to Wikileaks.org could potentially reveal the capabilities and vulnerabilities of US forces, whether stationed in CONUS or deployed overseas.

~~(S//NF)~~ The proliferation of access to Internet, computer, and information technology technical skills, software, tools, and databases will allow the rapid development, merging, integration, and manipulation of diverse documents, spreadsheets, multiple databases, and other publicly available or leaked information. Possible enhancements could increase the risk to US forces and could potentially provide potential attackers with sufficient information to plan conventional or terrorist attacks in locations such as Iraq or Afghanistan.

~~(S//NF)~~ The various open or freeware applications used in the development and management of Wikileaks.org continue to improve with time. Several Internet software development companies, foundations, electronic privacy organizations, database management services, encryption developers, and anonymous e-mail services can generate sufficient income, accept donations, and use volunteers to continue to develop and improve the software. Improvements in these software applications will provide greater privacy and anonymity of persons who leak information to Wikileaks.org.

~~(S//NF)~~ The possibility that various computer experts, researchers, and users could expand the data fields in the TOE SQL database to include pictures; equipment capabilities, limitations and vulnerabilities; known unit locations; links to geospatial information; and known unit personnel cannot be ruled out. The continued development of new technologies for merging and integrating various geographic or other information services into easy-to-use databases could allow rapid compilation of unit profiles that could be used for developing actionable information for use by FISS, foreign terrorist organizations, and other potential adversaries for intelligence collection, planning, or targeting purposes.[42]

[Back to Table of Contents]

(U) Point of Contact

(U) This special report was produced by the Army Counterintelligence Center (ACIC). ACIC POC is Michael D. Horvath, Senior Analyst, Cyber CI Assessments Branch, commercial, (b) (6) or DSN (b) (6).

[Back to Table of Contents]

(U) Appendix A: Glossary

(U) **FreeNet (or Freenet).** Freenet is a decentralized and censorship-resistant distributed data storage system. Freenet aims to provide freedom of speech through a peer-to-peer network with strong protection of anonymity. Freenet pools contributed bandwidth and storage space of member computers in the network to allow users to anonymously publish or retrieve various

kinds of data or information. The storage space is distributed among all connected nodes on Freenet.[43]

(U) **Google Earth**. Google Earth is a geographic information system (GIS) using the Google search engine that permits interactive viewing of digital satellite imagery, maps, terrain, and 3D buildings.[44]

(U) **MediaWiki.** Wikipedia runs on its own in-house-created software, known as MediaWiki, a powerful, open-source wiki system written in PHP and built upon MySQL. As well as allowing articles to be written, it includes a basic internal macro language, variables, transcluded templating system for page enhancement, and features such as redirection.[45]

(U) **OpenSSL.** The OpenSSL Project is a collaborative effort to develop an easy-to-use Open Source toolkit implementing the Secure Sockets Layer and Transport Layer Security protocols with encryption. The project is managed by a worldwide community of volunteers that use the Internet to communicate, plan, and develop the OpenSSL toolkit and its related documentation. The OpenSSL toolkit is licensed in a manner that allows free usage for commercial and noncommercial purposes subject to some simple license conditions. [46]

(U) **PGP.** PGP (Pretty Good Privacy) is an application and protocol for secure e-mail and file encryption developed by Phil Zimmerman. PGP was originally published as freeware, and the source code has always been available for public use and adaptation. PGP uses a variety of algorithms, such as IDEA, RSA, DSA, MD5, and SHA-1 for providing encryption, authentication, message integrity, and private and public-key management. PGP is based on the "Web-of-Trust" model and is the most popular encryption system used by individual personnel, businesses, and governmental entities throughout the world to protect or hide content on the Internet. [47]

(U) **SQL.** SQL (Structured Query Language) is also known as Database Language SQL (S-Q-L), is a computer language designed for the retrieval and management of data in a relational database management system, database schema creation and modification, and database object access control management. SQL is a standard interactive and programming language for getting information from and to update a database. Queries take the form of a command language that lets you select, insert, update, find out the location of data, and so forth. [48]

(U) **SQLite.** SQLite is a public domain software library that implements a self-contained, serverless, zero-configuration application that does not require setup or administration, cross platform, transactional SQL database engine that can support terabyte-sized databases and gigabyte-sized strings and blobs. SQLite is the most widely deployed SQL database engine in the world. The software application is used in countless desktop computer applications as well as consumer electronic devices including cellular phones, Personal Digital Assistants, and MP3 players. The source code for SQLite is in the public domain. SQLite is a popular choice as the database to back small-to-medium-sized Web sites because it requires no or little configuration and stores information in ordered disk files that are easy to access and will preserve transactions after system crashes or power outages. SQLite is a completely self contained application that has

a small code print (250KB size fully configured) and is a faster client/server for common operations. [49]

(U) **TOR (or Tor)**. Tor (The Onion Router) is a network of virtual tunnels that allows people or various groups to improve their privacy and security on the Internet. It also enables software developers to create new communication tools with built-in privacy features. Tor provides the foundation for a range of applications that allow organizations and individuals to share information over public networks without compromising their privacy. Using Tor protects you against a common form of Internet surveillance known as "traffic analysis." [50]

(U) **Traffic analysis**. Traffic analysis is a form of pattern and usage analysis that can be used to infer who sending or receiving e-mail and data exchanges on a private network, public network, or the Internet. Knowing the source and destination of Internet traffic allows individuals, criminals, law enforcement, and intelligence and security services to track the activities, behavior, and interests of the sender or receiver. This form of pattern analysis can be used to identify persons and possibly threaten a person's employment and physical safety by revealing who and where they are located. [51]

(U) **Web servers.** Web servers are computer hardware that stores HTML documents, images, text files, scripts, and other Web-related data, collectively known as content, and distributes this content to other clients on the network upon request.

(U) **Wiki.** A wiki is a type of Web site that allows users to easily add, remove, or otherwise edit and change some available content, sometimes without the need for registration. This ease of interaction and operation makes a wiki an effective tool for collaborative authoring. The term wiki can also refer to the collaborative software itself (wiki engine) that facilitates the operation of such a Web site or to certain specific wiki sites and the online encyclopedias such as Wikipedia. Wiki was created in 1994 and installed on the Web in 1995 by Ward Cunningham. [52]

(U) **Wikipedia**. Wikipedia is a blend of the words *wiki* and *encyclopedia*. Wikipedia is a multilingual, Web-based free content encyclopedia project operated by the nonprofit Wikimedia Foundation. Wikipedia is written collaboratively by volunteers, allowing most articles to be changed by almost anyone with access to the Web site. Wikipedia's main Web servers are in Tampa, FL, with additional Web servers in Amsterdam and Seoul.[53]

[Back to Table of Contents]

(U) Appendix B: Methodology Used by Authors for Analysis of Leaked Tables of Equipment for US Forces in Iraq and Afghanistan

(U) A Wikileaks.org staff writer, Julian Assange, with assistance from several other persons developed a SQL data base to store the 2,000 pages of leaked TOE information and merged information from other sources into a usable data base for research purposes. The entire SQL database developed by the authors for the TOEs was posted on the Wikileaks Web site for anyone to use. The following is a list of steps purportedly used to make the data easy to use and accessible for persons wanting to conduct their research.

1. Julian Assange and other persons that assisted him used publicly available open-source information to learn and understand the abbreviations, acronyms, numbers, and other nomenclatures in the leaked information, specifically NSN (NATO Stock Number), LIN (Line Item Number), and UIC (Unit Identification Code). The authors compiled their results and documented the information on US military logistics in a separate document on the Web site.

2. They then found various public NSN catalogues on the Internet, which were used to confirm the validity of random samples of the leaked information using these databases and other deployment references.

3. By hand, they created tallies for a select list of interesting items through their observations of the reviewed information within the database. They wrote a draft report based on their research and analysis of the database and other publicly available information.

4. They then used software and software applications such as VIM macros, PERL scripts, and several Python programs to organize the material into a more presentable spreadsheet format (such as Afghanistan OEF Property List and Afghanistan OEF Property List.html).

5. They wrote additional software code to merge data from several NATO Logistics spreadsheets, which allowed the NSNs to be organized into subcategories to identify the NATO Supply Group and NATO Supply Classification for the equipment.

6. They obtained a list of NATO Supply Group and NATO Supply Classification codes from public US military logistics sources available on the Internet that was merged with other spreadsheets.

7. They used SQL to install a database program.

8. They merged the original leaked data into group and classification code tables using a SQL database, in this case using SQLite. The authors noted that any SQL database could have been used to index and catalogue the information.

9. They used SQL to merge NATO Supply Classifications with leaked data to provide extra context and generate Afghanistan OEF Property List-extended.html.

10. Using SQL, they generated several different indexes and tallies for the leaked items, by NATO Supply Group, NATO Supply Classification, and NSN. This data was then converted into HTML format and placed into an appendix.

11. Again using SQL, they generated a unique list of NSNs. They wrote a script or software program to concurrently query the US logistics Web-query NSN search for pricing information and extract the price for every NSN on the list (except for alphanumeric NSNs, which are not listed, probably due to being Management Control Numbers).[54]

12. They merged pricing information into the SQL database.

13. They used SQL to generate a new tally by NSN, merged this with the pricing information for each NSN, sorted by the total price, converted the data to HTML, and placed it into the Appendix.

14. They used SQL to calculate the total value of all equipment for which they had cost information.

15. They examined the data and extracted additional information that was of interest such as notable units and items of equipment.[55]